
ZyWall 5 als Firewall im Netzwerk von SAI (Schulen ans Internet)

Anleitung zur Einstellung von ZyWall 5 als Router und Bridge

1. Einleitung:

Grundsätzlich wird das Netzwerk aller Schulen mit einem SAI-Anschluss durch die Firewall von Swisscom geschützt. Ausnahme sind die öffentlichen IP-Adressen (Web-, Mail-, Anwendungsserver, etc). Diese kurze Anleitung ist für SAI-1 Schulen gedacht, die mit einer eigenen Firewall ihre Schulgeräte zusätzlich schützen wollen (z. B. zusätzliche Websites sperren).

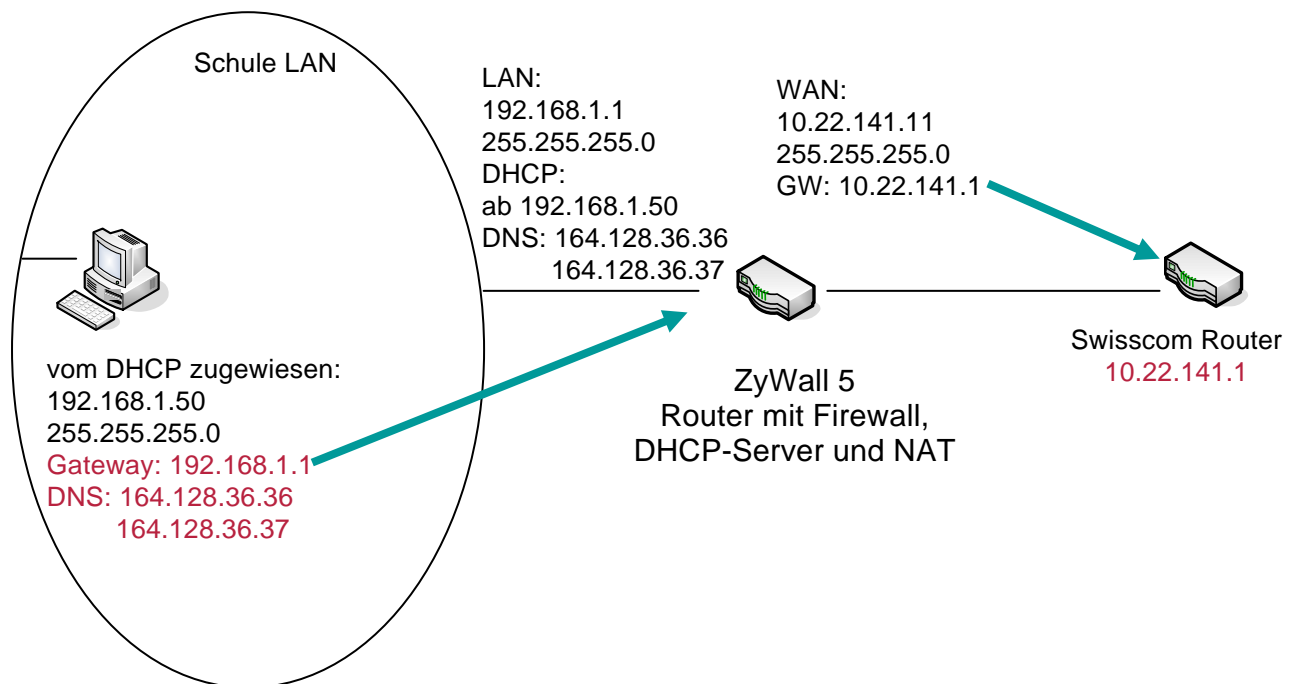
Im SAI-1 Netz haben Schulen aufgrund eigener Bedürfnissen eigene Firewalls eingerichtet. Viele dieser Firewalls sind standardmässig auf NAT (Network Address Translation) eingestellt. Weil gewisse Verbindungsprobleme mit Web- und Anwendungsservern auf NAT zurückzuführen sind, empfiehlt Swisscom, die eigene Firewall als transparente Firewall (auch Bridge genannt) einzustellen. Dies veranlasst uns zur Erstellung dieser kurzen Anleitung.

Die Anleitung zeigt die Einstellungen für die ZyWall 5 im Router- (NAT) und im Bridge Betriebsmodus.

Swisscom bietet einen VPN-Zugang für das SAI-1 Netz. Daher wird hier die Einstellung für VPN nicht erläutert.

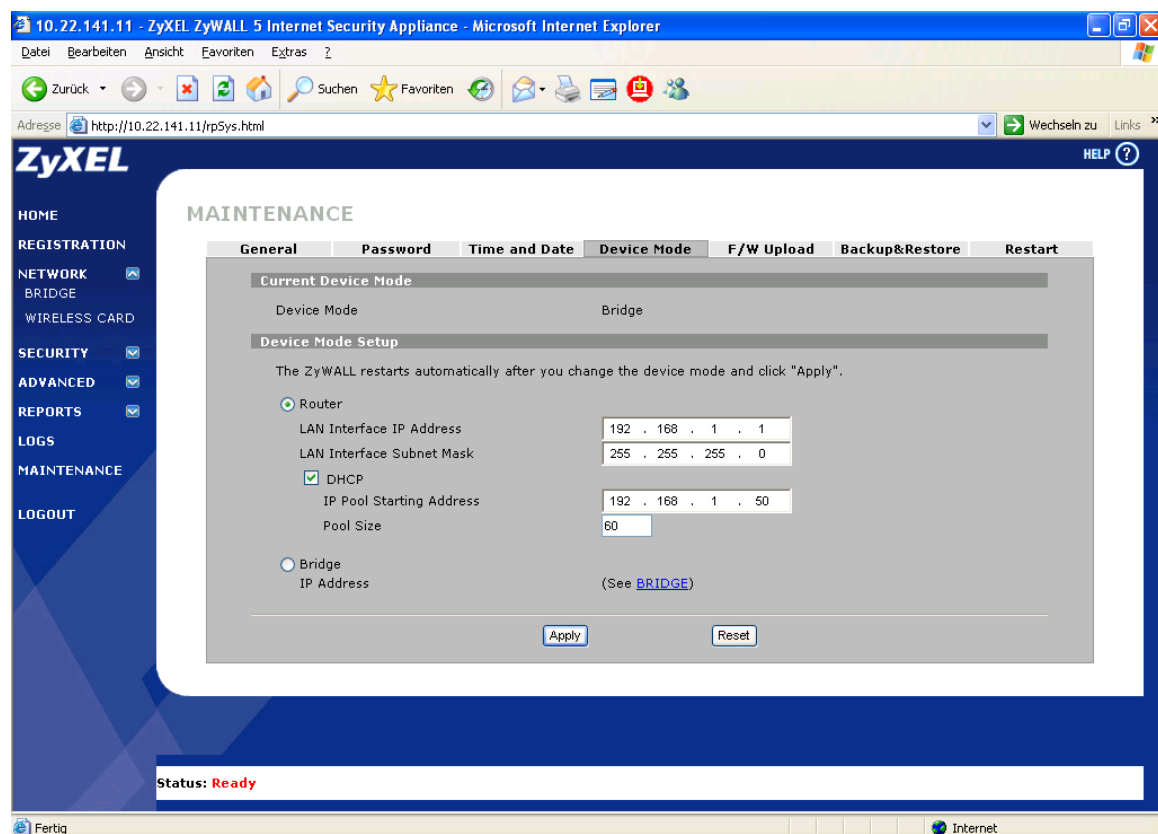
Anmerkung: Die ZyWall 5 bietet viele Funktionen an, die in einem produktiven Betrieb nützlich sind. Diese kurze Anleitung versteht sich nur als Empfehlung für die minimal benötigten Einstellungen um die ZyWall 5 als Firewall einzusetzen und kann das Benutzer-Handbuch nicht ersetzen. Um die umfassenden Funktionen der ZyWall 5 richtig einzusetzen, ist das Verständnis des Benutzer-Handbuchs unerlässlich.

2. Router Betriebsmodus:



2.1. ZyWall auf Router Betriebsmodus einstellen:

Menü "Maintenance" → "Device Mode"



2.2. WAN Anschluss einstellen:

Menü "Network" → "WAN"

The screenshot shows the ZyXEL ZyWALL 5 Internet Security Appliance web interface in Microsoft Internet Explorer. The browser address bar shows `http://192.168.1.1/rpSys.html`. The left sidebar contains a navigation menu with options: HOME, REGISTRATION, NETWORK (selected), LAN, WAN, DMZ, WLAN, WIRELESS CARD, SECURITY, ADVANCED, REPORTS, LOGS, MAINTENANCE, and LOGOUT. The main content area is titled "WAN" and has tabs for "Route", "WAN" (selected), "Traffic Redirect", and "Dial Backup". Under the "WAN" tab, there are three sections: "ISP Parameters for Internet Access" with "Encapsulation" set to "Ethernet" and "Service Type" set to "Standard"; "WAN IP Address Assignment" with "Use Fixed IP Address" selected, showing "My WAN IP Address" as 10.22.141.11, "My WAN IP Subnet Mask" as 255.255.255.0, and "Gateway IP Address" as 10.22.141.1; and "Advanced Setup" with "Enable NAT (Network Address Translation)" checked, "RIP Direction" set to "In Only", "RIP Version" set to "RIP-1", "Enable Multicast" unchecked, "Multicast Version" set to "IGMP-v1", "Spoof WAN MAC Address from LAN" unchecked, and "Clone the computer's MAC address - IP Address" set to 192.168.1.33. At the bottom left, the status is "Ready".

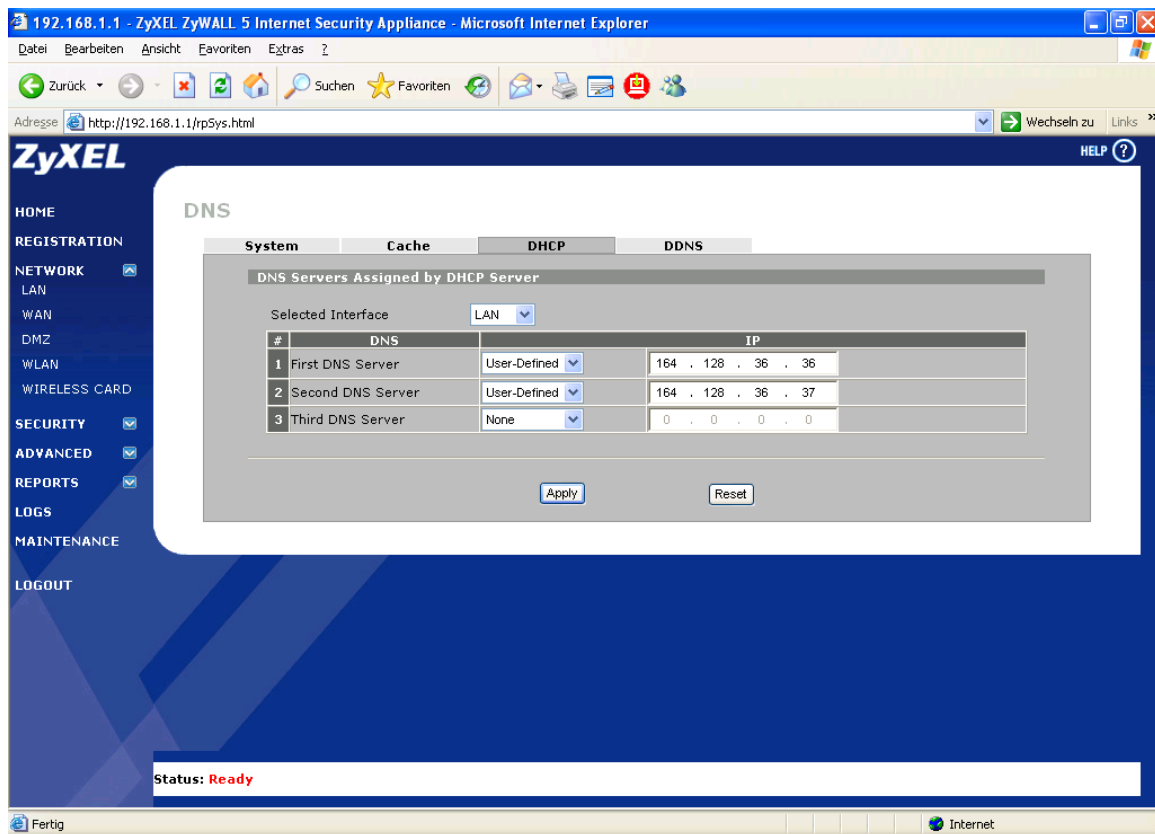
2.3. LAN Anschluss einstellen:

Menü "Network" → "LAN"

The screenshot shows the ZyXEL ZyWALL 5 Internet Security Appliance web interface in Microsoft Internet Explorer. The browser address bar shows `http://192.168.1.1/rpSys.html`. The left sidebar is the same as in the previous screenshot. The main content area is titled "LAN" and has tabs for "LAN" (selected), "Static DHCP", "IP Alias", and "Port Roles". Under the "LAN" tab, there are three sections: "LAN TCP/IP" with "IP Address" set to 192.168.1.1, "IP Subnet Mask" set to 255.255.255.0, "Multicast" set to "None", "RIP Direction" set to "None", and "RIP Version" set to "RIP-1"; "DHCP Setup" with "DHCP" set to "Server", "IP Pool Starting Address" set to 192.168.1.50, "DHCP Server Address" set to 0.0.0.0, "DHCP WINS Server 1" set to 0.0.0.0, "DHCP WINS Server 2" set to 0.0.0.0, and "Pool Size" set to 60; and "Windows Networking (NetBIOS over TCP/IP)" with three checkboxes: "Allow between LAN and WAN", "Allow between LAN and DMZ", and "Allow between LAN and WLAN", all of which are unchecked. A note states: "Note: You also need to create a [Firewall](#) rule." At the bottom, there are "Apply" and "Reset" buttons. At the bottom left, the status is "Configuration updated successfully".

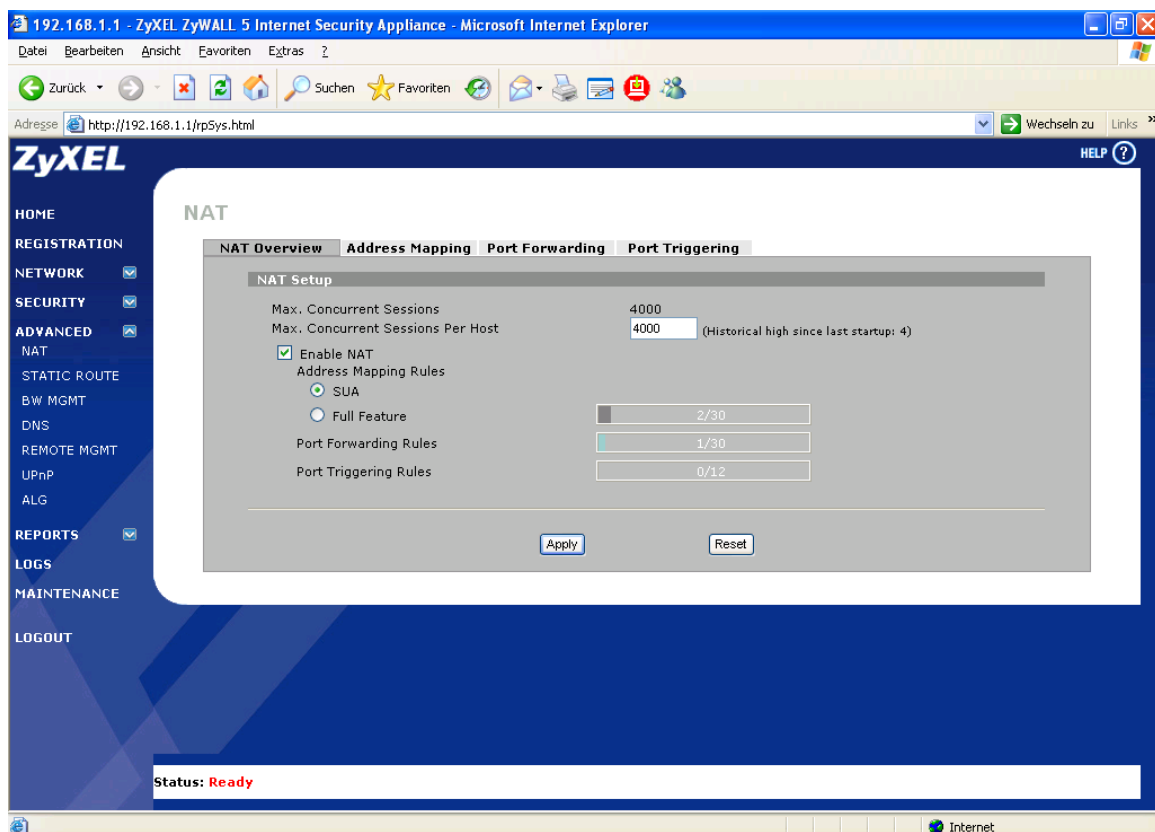
2. 4. DNS für DHCP einstellen:

Menü "Network" → "LAN" → "For DNS setup please click here"

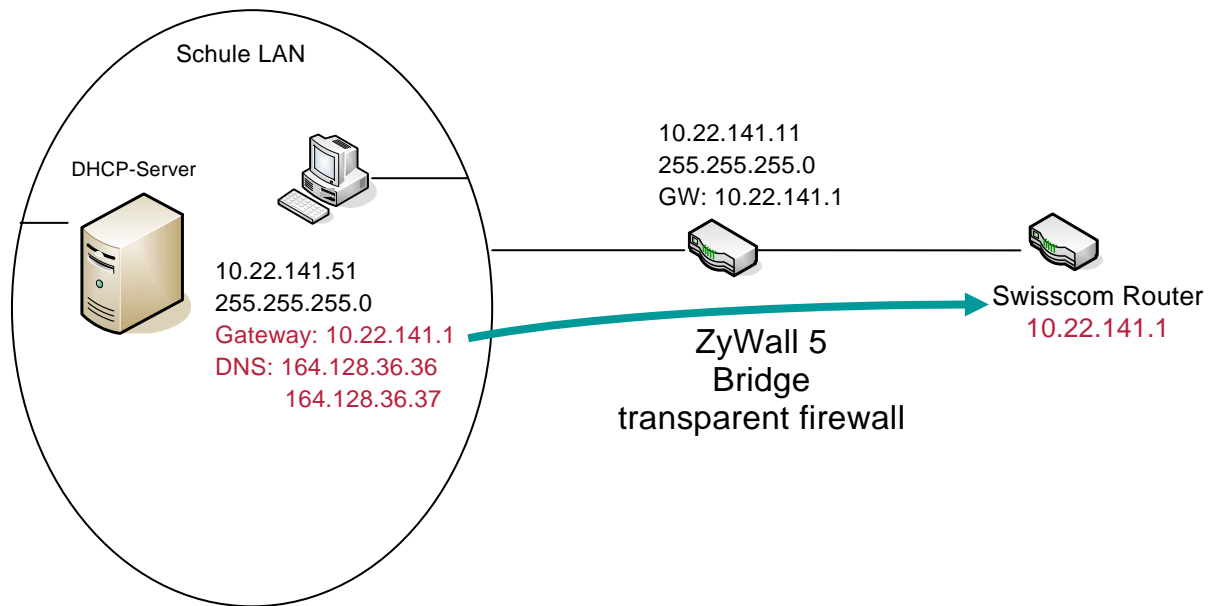


2. 5. NAT einstellen:

Menü "Advanced" → "NAT"

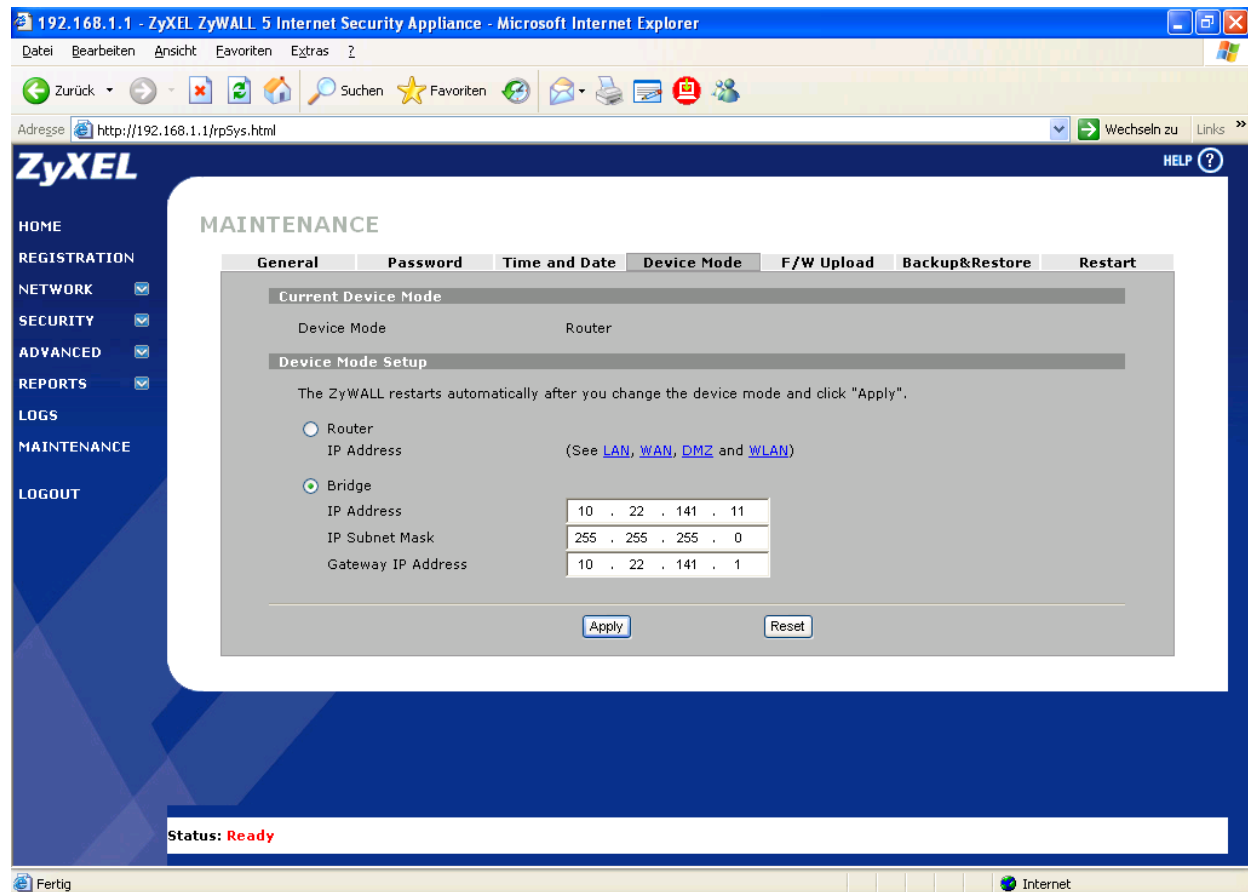


3. Bridge Betriebsmodus:



2.1. ZyWall auf Bridge Betriebsmodus einstellen:

Menü "Maintenance" → "Device Mode"



3.2. Bridge Parameter einstellen:

Menü "Network" → "Bridge"

BRIDGE

Bridge Setup

IP Address	10 . 22 . 141 . 11
IP Subnet Mask	255 . 255 . 255 . 0
Gateway IP Address	10 . 22 . 141 . 1
First DNS Server	164 . 128 . 36 . 36
Second DNS Server	164 . 128 . 36 . 37
Third DNS Server	0 . 0 . 0 . 0

Rapid Spanning Tree Protocol Setup

☐ Enable Rapid Spanning Tree Protocol

Bridge Priority	32768	0(Highest)~ 61440(Lowest)
Bridge Hello Time	2	1(Second)~ 10(Seconds)
Bridge Max Age	20	6(Seconds)~ 40(Seconds)
Forward Delay	15	4(Seconds)~ 30(Seconds)

Bridge Port	RSTP Active	RSTP Priority 0(Highest)~240(Lowest)	RSTP Path Cost 1(Lowest)~65535 (Highest)
WAN	<input type="checkbox"/>	128	250
LAN	<input type="checkbox"/>	128	250
Wireless Card	<input type="checkbox"/>	128	250
DMZ	<input type="checkbox"/>	128	250

Status: Ready

"Rapid Spanning Tree Protocol" wird nicht aktiviert. RSTP wird nur benötigt, falls im Netzwerk redundante Netzpfade als Backup für den Fehlerfall (Ausfall einer Strecke) verwendet werden.